Registered SQL Server Properties window - Privileged User Auditing tab

The Privileged User Auditing tab of the Registered SQL Server Properties window allows you to change the audit settings currently applied to privileged users on this SQL Server instance. You can choose to audit event categories and user defined events. An event category includes related SQL Server events that occur at the server level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

For example, you can audit individual SQL Server logins with privileged access, logins that belong to specific fixed server roles, all activities, or specific activities.

When you update audit settings to audit privileged user activities, these changes are not applied until the SQL trace is refreshed. The SQL trace is refreshed when the SQLcompliance Agent sends the trace files to the Collection Server. To ensure an immediate application of your new audit settings, click **Update Audit Settings Now** on the Agent menu.

SQL Server Extended Events support

Beginning with IDERA SQL Compliance Manager 5.4, SQL trace is deprecated as the product moves toward using SQL Server Extended Events. SQL Server Extended Events is an event handling system that offers lower overhead and delivers performance gains over the default SQL trace method. In SQL Compliance Manager 5.4, only SELECT and DML events for SQL Server 2012 and later versions are supported by this feature. All functionality that works on top of these events, such as DML/Select filtering, Before-After data, sensitive column auditing, and more, work with this new method of capturing event data.

There are two ways to enable Extended Event capture:

- using the using stored procedures

Users wanting to take advantage of SQL Server Extended Events auditing capabilities can do so on the Privileged User auditing tab of the registered SQL Server Properties window by selecting **Capture DML and Select activities using SQL Extended Events** in the Audited Activity area.

Available actions

Add

Allows you to select one or more privileged users to audit. You can select privileged users by login name or by membership to a fixed server role.

Remove

Allows you to remove the selected SQL Server login or fixed server role from the list of audited privileged users. When you remove the login or role, the SQLcompliance Agent no longer collects events recorded for that login or the role members.

Available fields

Privileged users and roles to be audited

Lists the audited privileged users by login name or fixed server role. ***If you are auditing privileged users in a fixed server role*** , the SQLcompliance Agent collects activities executed by all members of the selected role.

Audited Activity

Allows you to specify which activities (events) you want to audit for the selected privileged users. Select **Audit all activities done by privileged users** to include everything or select **Audit selected activities done by privileged users** followed by additional preferences for selective auditing. Available options include:

- Logins
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User defined events
- Filter events based on access check.

Capture DML and Select activities using SQL Extended Events *(available for only SQL Server 2012 and later versions)*

Allows you to specify whether you want to use Microsoft SQL Server Extended Events to collect SQL statements associated with audited database modification (DML) and Select activities. To capture these statements, you must also enable DML or Select auditing.

SQL Server Extended Events is a general event handling system that provides an alternate means to gather audit event data. Extended Events provide improved performance and a lower-overhead alternate to SQL trace (default method) when collecting DML of Select events.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture SQL statements for DML and SELECT activities

Allows you to specify whether you want to collect SQL statements associated with audited database modification (DML) and Select activities. To capture these statements, you must also enable DML or Select auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Capture SQL statements for DDL activities